Claims

We claim:

1. A method for providing a fair exchange of user information by encoding said information with a hidden value comprising the step of:

selecting said hidden value as one of a plurality of sequence values, wherein difference values between adjacent ones of said sequence values are symmetrically distributed about one of said values of a known order.

2. The method as recited in claim 1, wherein said difference values progressively increase then decrease about said value of known order.

3. The method as recited in claim 1, wherein said plurality of values are determined in accordance with a root value and a modulus value.

4. The method as recited in claim 1, wherein said sequence values are determined as:

$$\left(g^{2^{2^i}}\right)_{i=0}^{K} \bmod(N);$$

$$\left(g^{2^{((2^K+1)-(2^K-n))}}\right)_{n=1}^{K} \bmod(N);$$

where K is a known order;
N is a modulus value; and
g is a root value.

5. The method as recited in claim 4, wherein said sequence further comprises the values:

$$g \quad \text{and} \quad g^{2^{2^K+1}} \bmod(N).$$

6. The method as recited in claim 4, wherein said modulus value is selected from the group consisting of Blum integers in the form of $N = p_1 p_2$.

7. The method as recited in claim 6, wherein said Blum integers are selected from the group satisfying:

$$p_1 = 2q_1 + 1; and$$
$$p_2 = 2q_2 + 1$$

wherein q_1 and q_2 are prime numbers.

8. The method as recited in claim 7, wherein a period of a sequence in the form of $2^i \bmod(q_1 q_2)$ is at least 2^{500}.

9. The method as recited in claim 1, wherein said hidden value is selected as a value immediately preceding a last value of said sequence.

10. The method as recited in claim 1, wherein said order value of known order is at least 80.

11. A method for exchanging user information over a network comprising the steps of:

transmitting over said network said user information encoded in association with a hidden value selected as one of a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order;

transmitting over said network a first set of said values and a last value in said sequence, wherein said values in said first set have increasing differences between adjacent ones of said values; and

transmitting, individually, said remaining values in said sequence.

12. The method as recited in claim 11, wherein said remaining values are transmitted in response to a received information item.

13. The method as recited in claim 11, wherein said remaining values are transmitted on a timed-basis.

14. The method as recited in claim 11, further comprising the steps of:

associating a validation value with each of said plurality of values; and

transmitting said validation value.

15. The method as recited in claim 14, wherein said validation values are transmitted concurrently with said associated value.

16. The method as recited in claim 14, wherein said validation values are transmitted sequentially with said associated value.

17. The method as recited in claim 11, further comprising the steps of:

determining said hidden value; and

decoding said user information.

18. The method as recited in claim 11, wherein said plurality of values are determined as:

g ;

$\left(g^{2^{2^i}}\right)_{i=0}^{K} \bmod(N)$;

$\left(g^{2^{((2^K+1)-(2^K-n))}}\right)_{n=1}^{K} \bmod(N)$; and

$g^{2^{2^K+1}} \bmod(N)$

where K is said order value;
N is a modulus value; and
g is a root value;

19. The method as recited in claim 18, wherein said modulus value is selected from the group consisting of Blum integers in the form of $N=p_1p_2$ wherein

$$p_1 = 2q_1 + 1; and$$
$$p_2 = 2q_2 + 1$$

wherein q_1 and q_2 are prime numbers

20. The method as recited in claim 18, wherein a period of said sequence in the form of 2^i mod(N) is at least 2^{500}.

21. The method as recited in claim 11, wherein said hidden value is a value immediately preceding said sequence last value.

22. The method as recited in claim 11, wherein said known order is at least 80.

23. A system for exchanging user information over a network comprising:

a processor in communication with a memory, said processor operable to execute for:

transmitting over said network said user information encoded in association with a hidden value selected as one of a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order;

transmitting over said network a first set of said values, and a last value in said sequence, wherein said values in said first set have increasing differences between adjacent ones of said values; and

transmitting, individually said remaining values.

24. The system as recited in claim 23, wherein said processor is further operable to execute code for transmitting said remaining values in response to a received information.

25. The system as recited in claim 23, wherein said processor is further operable to execute code for transmitting said remaining values on a timed-basis.

26. The system as recited in claim 23, wherein said processor is further operable to execute code for:

associating a validation value with each of said plurality of values; and

transmitting said validation value wherein said validation values may be transmitted concurrently with or sequentially to said associated value.

27. The system as recited in claim 23, wherein said processor is further operable to execute code for:

determining said hidden value; and

decoding said user information.

28. The system as recited in claim 23 further comprising:

an input/output device in communication with said processor and said network operable to exchange information between said processor and said network.

29. The system as recited in claim 23 wherein said code is stored in said memory.